411 Individual HW7

Jack Madden

November 2023

Problem 1

a) We have that $\langle 6 \rangle$ is the kernel of the homomorphism $\phi : \mathbb{Z}_{24} \to \mathbb{Z}_6$, $\phi : x \to x\ mod\ 6$. The image of $\mathbb{Z}_2 4$ under this homomorphism is the numbers 0 through 5. Thus we see that quotient group has order 6 and its cosets are $\langle 6 \rangle, 1 + \langle 6 \rangle, 2 + \langle 6 \rangle, 3 + \langle 6 \rangle, 4 + \langle 6 \rangle, 5 + \langle 6 \rangle$.

b) We have that $SL_n(\mathbb{R})$ is the kernel of the homomorphism $\phi : x \to det(x)$, $\phi : GL_n(\mathbb{R}) \to \mathbb{R}^*$. The image of $GL_n(\mathbb{R})$ is all of $\mathbb{R}^*$. Then the quotient group is isomorphic $\mathbb{R}^*$ and has cosets of the form $aSL_n(\mathbb{R})$, $a \in \mathbb{R}^*$.

Problem 2

a) The key observation here is that every continuous bijection $\mathbb{R} \to \mathbb{R}$ must be monotonically increasing or decreasing, as otherwise it will not be injective and therefore not a bijection. Also, without this condition, a function could be bounded and therefore not surjective. Thus, we proceed to show that the set described under composition is a subgroup.

The function $y = x$, which is monotonically increasing, is the identity. To check that inverses are in the set, suppose we have a function f in the set. Let f be monotonically increasing. Then $f(x_1) < f(x_2)$ for any $x_1, x_2 \in \mathbb{R}$ such that $x_1 < x_2$. Thus, for any $f(x_1) < f(x_2)$, we will have $x_1 < x_2$ and therefore f^{-1} will also be monotonically increasing. Then let f be monotonically decreasing. So $f(x_1) > f(x_2)$ for $x_1 < x_2$. Then for any $f(x_2) < f(x_1)$, $x_2 > x_1$ and f^{-1} will be monotonically decreasing. Finally we must show that the group is closed under composition. Say we have a monotonically increasing function f, and a function g in the set. Consider $f \circ g$. If g is monotonically increasing, then walking positively along g will produce a set of increasing numbers which when passed up to f will produce a set of increasing real numbers. Then let g be monotonically increasing. Walking positively along g will pass up a set of decreasing numbers to f which will produce a set of decreasing numbers. Thus, a monotonically increasing function composed with either an increasing or decreasing function produces another increasing or decreasing function. A similar closure follows when f is monotonically decreasing. SO it is a subgroup.

b) We show that $\text{Isom}(\mathbb{R}^n)$ is a subgroup. First, we see that it has the identity element e which sends every point in $\mathbb{R}^n$ to itself. This clearly preserves distances, as $|y - x| = |y - x|$ for any $x, y \in \mathbb{R}^n$. Next, we show that if $f \in Isom(\mathbb{R}^n)$, this implies that $f^{-1} in Isom(\mathbb{R}^n)$. We know that for any two points in the image of f, which is simply R^n of equal distance, f^{-1} will map them to two points of equal distance in the domain of f, which is also R^n. So f^{-1} preserves the distances between any two points in its domain (image of f, R^n), and its range (domain of f, R^n). So f^{-1} is also in $Isom(\mathbb{R})$. Finally we need to check that the composition of two isometries is also an isometry. We have that for any $x, y \in \mathbb{R}^n$, $|f(y) - f(x)| = |g(y) - g(x)| = |y - x|$ for $f, g \in \text{Isom}(\mathbb{R}^n)$. Let $f(x) = x_1, f(y) = y_1$. Then x_1 and y_1 are the same distance as x and y. Then $g(x_1)$ and $g(y_1)$ are also the same distance apart as x_1 and y_1 and transitively the same distance aparty as x and y. So $|g(f(y)) - g(f(x))| = |y - x|$ for any points in $\mathbb{R}^n$ and thus $g \circ f \in \text{Isom}(\mathbb{R}^N)$ and so it is closed under composition.

Problem 3

a) We see that the function which maps all monotonically increasing functions to 0 and all monotonically decreasing functions to 1 is a homomorphism from $S_{\mathbb{R}}^0$ to $\mathbb{Z}_2$. This structure preserving behavior was shown in the closure section of 2b i.e. let f_1, f_2 be increasing and g_1, g_2 decreasing,

$$\phi(f_1 \circ f_2) = 0 = 0 + 0 = \phi(f_1) + \phi(f_2)$$

$$\phi(f_1 \circ g_1) = 1 = 0 + 1 = \phi(f_1) + \phi(g_1)$$

$$\phi(g_1 \circ f_1) = 1 = 1 + 0 = \phi(g_1) + \phi(f_1)$$

$$\phi(g_1 \circ g_2) = 0 = 2 \equiv 0 \ mod\ 2 \ = 1 + 1 = \phi(g_1) + \phi(g_2)$$

b) We see that the function which maps all rotations and translations to 0 and all reflections to 1 is a homomorphism from Isom($\mathbb{R}^n$) to $\mathbb{Z}_2$. This is because the composition of rotations is a rotation, the composition of translations is a translation, and the composition of a rotation and translation is a rotation with a translation. But the composition of a reflection with a rotation is a reflection, a reflection with a translation a reflection, but a reflection with a reflection is a rotation. This structural property within Isom($\mathbb{R}^n$) gives the described homomorphism.

Problem 4

a) For $x, y \in G$, $\phi(x) + \phi(y) = nx + ny$. Since G is abelian, this becomes $n(x + y) = \phi(x + y)$, and thus ϕ is a homomorphism.

b) Since H is cyclic, it is either isomorphic to $\mathbb{Z}_n$ for some finite n, or $\mathbb{Z}$.

Suppose that H is isomorphic to $\mathbb{Z}_n$. Then every element in H can be written as h^m, $0 \leq m < n$ where h is a generator in H. We then have that for any $(h^m, k) \in H \times K$, we have that $\phi_{|H|}((h^m, k)) = ((h^{|H|})^m, k^{|H|}) = (e, k^{|H|})$. Thus, we then have that $\phi_{|H|}(H \times K) \subseteq H \times K$ if H is not the trivial group. Then, since every element in g is isomorphic to an element in $H \times K$, we have that the image of G under the homomorphism $\phi_{|H|}$ will be the subgroup of G isomorphic to $\{(e, k_1^{|H|}), (e, k_2^{|H|}, \dots, (e, k_i^{|H|})\}$. If H is not trivial, there will be elements in G which map to elements of the form (h^m, k), $m \neq 0$, and then $\phi(G) < G$.

Suppose that H is isomorphic to $\mathbb{Z}$. Then every element in H can be written as h^m, $m \in \mathbb{Z}$ and thus every element in $H \times K$ is (h^m, k), $k \in K$. We then observe that the image of $H \times K$ under ϕ_2 is $\{\cdots, (h^{-4}, k_1^2), (h^{-2}, k_2^2), (e, k_3^2), (h^2, k_4^2), (h^4, k_5^2), \cdots\}$. Since the image of $H \times K$ under a homomorphism is isomorphic to the image of G under a homomorphism, this is isomorphic to the subgroup of elements in G which map to elements of the form (h^{2m}, k), $m \in \mathbb{Z}, k \in K$. But since there is an element in g which maps to (h, k), which is not in the image, it will not be in $\phi(G)$. Thus $\phi_2(G) < G$.

c) For this, we observe that $\phi_n(\mathbb{Q}) = \mathbb{Q}$ for any n. We show this by contradiction. Suppose $\frac{k}{m} \in \mathbb{Q}$ and $\frac{k}{m} \notin \phi_n(\mathbb{Q})$ for some n. But $\frac{k}{mn} \in \mathbb{Q}$, and then $\phi_n(\frac{k}{nm}) = \frac{k}{m}$ which implies $\frac{k}{m} \in \phi_n(\mathbb{Q})$. Contradiction.

From part b we have that $\phi_n(G) = G$ for any n implies that G is not isomorphic to the direct product of $H \times K$, where H is some cyclic group. Any direct product of cyclic groups can be written in the form $H \times K$, where H is one component of the direct product and K is the direct product of the rest of the components. So $\mathbb{Q}$ cannot be written as the direct product of cyclic groups.

Problem 5

a) We examine this group component by component to find the kernel. Take an arbitrary component $Z_{p^{n_i}}$. For $x \in Z_{p^{n_i}}$, define $\phi_p(x) = px$. If x in the kernel, then $px = \ell p^{n_i}$ for some $\ell \in \mathbb{Z}$. We then have $x = \ell p^{n_i - 1}$, and observe that $ker(\phi_p)$ is the set of multiples of p^{n_i-1} mod p^{n_i}, which are $0, p^{n_i-1}, 2p^{n_i-1}, 3p^{n_i-1}, \cdots (p-1)p^{n_i-1}$. This finding is easily extended to the direct product. We then define an isomorphism f from $(\mathbb{Z}_p)^k$ to H as follows. For $(x_1, x_2, x_3, \cdots x_k) \in (\mathbb{Z}_p)^k$,

$$f((x_1, x_2, x_3, \cdots, x_k)) = (x_1 p^{n_1-1}, x_2 p^{n_2-1}, x_3 p^{n_3-1}, \cdots x_k p^{n_k-1})$$

We will now show that f is an isomorphism, by showing injectivity, surjectivity, and the homomorphism property: Let

$$(x_1 p^{n_1-1}, x_2 p^{n_2-1}, \cdots x_k p^{n_k-1}) = (y_1 p^{n_1-1}, y_2 p^{n_2-1}, \cdots y_k p^{n_k-1})$$

We take an arbitrary component. Let $x_i p^{n_i-1} = y_i p^{n_i-1}$. Then $x_i = x_i \frac{p^{n_i-1}}{p^{n_i-1}} = y_i$. So $f((x_1, \ldots, x_k)) = f((y_1, \ldots, y_k)) \rightarrow (x_1, \ldots, x_k) = (y_1, \ldots, y_k)$. For surjectivity, since H is a vector multiples of p^{n_i} mod p_i^n and $(\mathbb{Z}_p)^k$ is a vector of numbers $0, 1, \ldots, p-1$, there will always be $x \in (\mathbb{Z}_p)^k$ such that $f(x) = h$ for any $h \in H$.

Last, we show the homomorphism property.

$$f((x_1, \ldots, x_k) + (y_1, \ldots, y_k)) = ((x_1 + y_1)p^{n_1-1}, \ldots, (x_k + y_k)p^{n_k-1}) = (x_1 p^{n_1-1} + y_1 p^{n_1-1}, \ldots, x_k p^{n_k-1} + y_k p^{n_k-1})$$

$$= (x_1 p^{n_1-1}, \ldots, x_k p^{n_k-1}) + (y_1 p^{n_1-1}, \ldots, y_k p^{n_k-1}) = f((x_1, \ldots, x_k)) + f((y_1, \ldots, y_k))$$

b) We do this component by component. We see that the quotient group $\mathbb{Z}_{p^{n_i}}/\mathbb{Z}_p$ must be cyclic, as it is a quotient of a cyclic group. It will also have order p^{n_i-1}, by Lagrange's theorem. Thus the quotient of each component is isomorphic to $\mathbb{Z}_{p^{n_i}-1}$. Then, we have that the quotient G/H is isomorphic to $\mathbb{Z}_{p^{n_1-1}} \times \ldots \times \mathbb{Z}^{p^{n_k-1}}$, which is isomorphic to K by the first isomorphism theorem.

c) We know that G is a finitely generated Abelian group, as it can be generated by k generators

$$(1, 0, \ldots, 0), (0, 1, 0, \ldots, 0), \cdots, (0, 0, \ldots, 0, 1)$$

. Thus it is isomorphic to some direct product of cyclic groups with orders of powers of primes by the Fundamental Theorem of finitely generated abelian groups. But G is the group yielded by this theorem itself exactly. The theorem states that this group is unique, up to permutation of components. But since we have defined an ordering, these components are determined exactly uniquely.

Problem 6

We first look at the stabilizer of the identity. The orbit of the identity is just itself, as conjugating the identity by anything yields just the identity. By the orbit stabilizer theorem, we know that its stabilizer must be a subgroup of order 12, and therefore its stabilizer is A_4 itself.

Next, we look at the pairs of transpositions. We observe that $Orb((1\ 2)(3\ 4))$ is the conjugacy class of pairs of cycles. This is because $(1\ 3\ 2)(1\ 2)(3\ 4)(1\ 2\ 3) = (1\ 3)(2\ 4)$ and $(1\ 2\ 3)(1\ 2)(3\ 4)(1\ 3\ 2) = (1\ 4)(2\ 3)$. We observe that the orbit cannot be any larger as the cycle structure will not change under conjugation. Also since orbits are equivalence classes, the other elements of the conjugacy class have the same orbits. From this, we have that the orbit of these elements has order 3, and since the order of the group is 12, the stabilizer must have order 4. Since the stabilizer is a subgroup, and only the V_4 subgroup of A_4 has order 4, the stabilizer of these elements must be V_4.

Next, we look at the the 3-cycles. After some computation we find that they are broken down into 2 orbits of order 4, $\{(1\ 2\ 3), (1\ 3\ 4), (2\ 4\ 3), (1\ 4\ 2)\}$ and $\{(1\ 3\ 2), (2\ 3\ 4), (1\ 2\ 4), (1\ 4\ 3)\}$. This implies that the stabilizer of a 3 cycle has order 3 from orbit stabilizer theorem. The only subgroups with order 3 in A_4 are subgroups composed of the identity, a 3-cycle, and its inverse. Thus, we have that the stabilizer for every 3 cycle is the subgroup composed of the identity, itself, and its inverse.

Problem 7

a) To do this we must show that the group axioms hold. First, for any set in the power set $\{i_1, \cdots, i_k\}$, if e is the identity permutation in S_n, $e \cdot \{i_1, \cdots, i_k\} = \{e(i_1), \cdots, e(i_k)\} = \{i_1, \cdots, i_k\}$. So the identity axiom holds. We must then check that the group action is associative. If we consider an aribtrary member i_j of the arbitrary subset $\{i_1, \cdots, i_k\}$, and the arbitrary permutations $\sigma_1, \sigma_2 \in S_n$, we have that $\sigma_1(\sigma_2(i_j)) = \sigma_1 \circ \sigma_2(i_j)$ as this is how function composition works. So the group action is well defined.

b) We observe that for any element in the power set of size k, it can be "relabeled" by some permutation in S_n to form any element of size k in the power set. Based on this, there are $n+1$ orbits in the power set, with the 1 added due to the empty set.

c) Let's find the stabilizer of $\{1, \cdots, k\}$. If we have $\sigma \cdot \{1, \cdots, k\} = \{1, \cdots, k\}$ for some $\sigma \in S_n$, it means we have $\sigma(1) \in \{1, \cdots, k\}, \sigma(2) \in \{1, \cdots, k\}, \cdots, \sigma(k) \in \{1, \cdots, k\}$, and also $\sigma(k+1) \in \{k+1, \cdots, n\}, \sigma(k+2) \in \{k+1, \cdots, n\}, \cdots, \sigma(n) \in \{k+1, \cdots, n\}$. We can count the number of these permutations that exist by noting that σ has k ways to map 1, $k-1$ ways to map 2, and so on. We then note that there are $n-k$ ways to map $k+1$, $n-k-1$ ways to map $k+2$, and so on. Thus we have characterized the stabilizer. The size of the stabilizer of an element of size k is then $(n-k)!k!$

d) We have that the size of S_n is $n!$, and the size of the stabilizer of an element of size k is $(n-k)!k!$. From the orbit-stabilizer theorem we have that the size of the orbit of an element of size k is then $\frac{n!}{(n-k)!k!}$. This is just $\binom{n}{k}$, which makes sense.

Problem 8

We know that since the action is transitive, there exists an element $g \in G$ such that $g \cdot y = x$. We content that for this element g, $G_y = g^{-1}G_xg$. We have:

$$y = y$$

$$g \cdot y = g \cdot y$$

we choose arbitrary $h \in G_x$:

$$g \cdot y = hg \cdot y$$

$$g^{-1}g \cdot y = g^{-1}hg \cdot y$$

$$y = g^{-1}hg \cdot y$$

This implies that for any $h \in G_x$, $g^{-1}hg \in G_y$, which implies that $g^{-1}G_xg \subseteq G_y$. To prove that $G_y \subseteq g^{-1}G_xg$, we must show that for any $k \in G_y$, there exists $h \in G_x$ such that $k = g^{-1}hg$, or $gkg^{-1} = h$. We have:

$$x = x$$

$$g^{-1} \cdot x = g^{-1} \cdot x$$

Choose arbitrary $k \in G_y$

$$g^{-1} \cdot x = kg^{-1} \cdot x$$

$$x = gkg^{-1} \cdot x$$

Since this implies that gkg^{-1} is a stabilizer of x, we know that there exists some $h \in G_x$ such that $gkg^{-1} = h$. So then we have $G_y \subseteq g^{-1}G_xg$, and $G_y = g^{-1}G_xg$.

Problem 9

a) We start by defining the rotations of the cube. In every rotation of the cube, one of the 6 faces will be on top. Once this face is selected, there are 4 ways the cube can be rotated. Since each of the top 4 corners is affixed to a corresponding bottom corner, once the top 4 corners are determined the cube is fixed. So we can see that any rotation of the cube can be thought of as a choice of top face and a rotation about the axis going through that face and the opposite face. We will have then diagonals, a, b, c, d, which will themselves have corners $a_1, a_2, b_1, b_2, c_1, c_2, d_1, d_2$.

b) We describe the stabilizer of a diagonal x. Suppose that x_1 is the corner that is on top in the start position and x_2 is the corner that is on the bottom. When x_1 is in its start position, the cube can be held still, rotated 120 degrees about the diagonal, or rotated 240 degrees about the diagonal. Likewise, x_2 can be placed x_1's start position on top, by a rotation by 180 degrees about the axis between the midpoints of two opposite edges, held still, or rotated by 120 or 240 degrees. This gives 6 elements in the stabilizer which makes sense, as the group has order 24 and the diagonals constitute one orbit of order 4. If an element other than the identity (holding x_1 in its start position and not moving) holds all diagonals constant, one of these 6 rotations must do that. However, we see that the 4 rotations by 120 and 240 move 3 diagonals, and the one rotation which swaps x_1 and x_2 moves 2 diagonals. Thus, the only rotation in the stabilizer of any element that holds all diagonals constant is the identity itself. So the intersection of the stabilizers will just be the identity.

c) We see that every rotation applied to all the diagonals constitutes a bijection, as 4 diagonals are moved to 4 diagonals, and no two diagonals are moved to the same place (would deform the cube). We see that it has an identity, and that every rotation has an opposite(inverse) rotation, and that two rotations will always go to another rotation as each individual rotation preserves the orientation of the cube. So we know that G is isomorphic to some subgroup of S_4 but G has order 24, so since it is isomorphic to a subgroup with order 24, it is isomorphic to S_4 itself.